REMARKS

This paper is in response to the Office Action of December 14, 2005. Reconsideration is requested.

The Examiner is thanked for the telephone conference of February 9, 2006 and February 10, 2006. A discussion was had regarding the contents of the main reference to Uranaka et al. (US 6,470,085). It was pointed out to the Examiner that many of functional elements are not disclosed nor suggested by the steps performed in Uranaka et al.

The Examiner alleged that the claims of the present invention do not require the operations to be performed in order, and therefore, the Examiner is free to locate similar features in disparate sections of Uranaka et al. to suggest the claimed elements of Applicants' claim invention. The undersigned respectfully disagrees.

The claimed invention is defined by the claimed operational elements, and each successive operation identified in the claim is linked to prior operations. Reading the claims otherwise would simply be illogical. For instance, it is not possible to use a user key pair before it is created or exchanged, it is not possible to use a console key pair before it is created or exchanged, and it is not possible to obtain double encryption for the software title if the prior levels of encryption have not been created at the specified and claimed sides between the server and console computers. Consequently, the Applicants submit that the Examiner's assertion that each of the elements in the claims can be practiced in any order is technically incorrect. Further, it is respectfully submitted that it is improper to use hindsight to reconstruct the claimed invention by picking an choosing from the multiple embodiments of Uranaka et al.

Additionally, one skilled in the art reading the teachings of Uranaka et al. would not be motivated to construct the claimed methodology defined in the independent claims, as Uranaka et al. uses different procedures for ensuring security of its distributed application package.

As Uranaka et al. fails to teach each of the elements alleged to be taught by the Office, the general teachings of the secondary reference would fail to cure the combined deficiencies. Additionally, as noted in the prior office action response, the secondary reference to Schneier is broadly concerned with the basics of communication using Public-Key Cryptography (PKC). The Applicants' invention is not attempting to claim PKC *per se*, but alternatively, the use of PKC in accordance with a specific and unique methodology, as defined in the independent claims. PKC technology is a basic building block, which analogously is similar to a transistor being a basic building block. In a circuit invention, a new circuit will necessary use transistors, but the fact that transistors are used does not obviate the novelty of the new circuit.

In the following table, an analysis of claim 88 is made in comparison to the teachings of Uranaka et al. is provided. Similar elements are present in independent claims 94, 100, and 106. Accordingly, the arguments presented for representative claim 88 equally apply to the remaining independent claims. Even though the undersigned appreciates that the rejection is under Section 103, a feature-by-feature analysis of Uranaka et al. will show that many of the elements noted by the Office to be present in Uranaka et al. are actually missing and in some cases, contradicting the claimed elements of the present invention.

Table A:

88. (previously presented) A method for enabling access to a software product, communication to enable the access to the software product being between a user computer and a server computer, the user computer executing program instructions to enable the method, comprising:	The Office cites col. 8, lines 34-41. This teaching defines *recording* a specific public key on a DVD. It is noted that the public key can be recorded on the DVD for multiple family members. However, this recording is done by the manufacturer. See Col. 18, lines 54-61. Uranaka et al.'s teaching fails to define *accessing* a software product that is present or made available by a server computer. The teaching "records" the public key directly on "a DVD."
initiating access to the server computer, the initiating causing creation of a user public key and a user private key defining a user key pair at the server computer,	The Examiner cites Col. 4, lines 44-65 and Col. 3, lines 30-45. Column 3 is only a brief description of drawings. The cited sections in column 4 defines charged information can

	be on a package (e.g., disc) or online. For online, this section simply teaches that charged information is transmitted to a user, but nowhere discusses initiating access to *cause* "creating a user public key and a user private key." The Examiner also cites to Col. 8, lines 34-41, to allege that server key pairs are generated at the server based on user information. This section, in fact refers to Fig. 7 of Uranaka. It is noted in the cited section that a "server public key Pks" that is in server table 75 is stored in EEPROM 103 of the user computer. The table 75 is used for associating the PKs contained in the distribution descriptor 23 recorded in the burst cutting area of the DVD with the ID and the network address. In the Applicants' claims, the user public key and a user private key defining a user key pair are created at the server, and are created using the user information. (also see next clause in the Applicants claims). The Applicants submit that Col. 8 says nothing about *causing* the *creation* of a user public key and a user private key defining a user key pair *at the server computer*, in response *initiating access*. The Examiner further cites col. 7, lines 1-9. This teaching having a person "*notify*" his or her public key Pku corresponding to his or

	her secrete key to a server, so the DVD manufacturer can record it onto the DVD. There is no teaching of "*creating*" a user public key and user private key, which is "*caused*" by the initiation of access to the server computer. To the contrary, the server/manufacturer in Uranaka et al. is "obtaining" a Pku from a user, not *creating* a Pku.
the server computer communicating the user public key to the user computer, and the user key pair being generated using information from a specific user;	As noted above, the user is "notifying" the DVD maker of his Pku. In the claims, the server computer "*generates*" the user public key and the user public key. Consequently, the teachings of Uranaka et al. are teaching to perform an act that is not useful or contrary to what is claimed. In the claimed invention, the server does not need to be notified of the Pku, as the sever is the one generating the Pku.
creating at the user computer, a console public key and a console private key defining a console key pair;	The Examiner cites Columns 19 and 15 (among others). The Applicants respectfully submit that the Office is combining the reasoning of the "user key pairs" and the "console key pairs" in the same analysis. As noted in the Office Action, the examiner is equating the user key pairs noted in Uranaka et al. with the "console key pair". However, as claimed, the function use of the user key pairs and the console key pairs are different and are used at different steps in the claimed processes. Consequently, Uranaka et al. fails to teach the functionally of the console key pairs.
sending the console public key to the server computer,	Because Uranaka et al. does not generate

	console key pairs, this step is missing from the art.
the console public key being encrypted using the user public key;	Because Uranaka et al. does not generate console key pairs, this step is missing from the art. Reference is again made to Column col. 7, lines 1-9, as noted by the Examiner. This teaching requires a person to "*notify*" his or her public key Pku corresponding to his or her secrete key to a server, so the DVD manufacturer can record it onto the DVD. Notice that in the claims, when the console public key is sent to the server computer, the console public key is encrypted using the user public key. This is not the case in Uranaka et al.. When the Pku is notified, it is not itself subjected to encryption. This is contradictory to this operation of the claimed invention.
forwarding a title ID to the server computer to enable access to the software product that is encrypted using a title public key, the title ID being encrypted using the user public key;	The Office cites to columns 22, 18, 19, and 24. Specifically, column 18, lines 25-27 describes having the "application " distributed via transmission media. In this model, the control program is transmitted with the application, which is stored on the user's hard drive. Note that this embodiment is not the same as the one where the program is on the DVD and the control program is also on the DVD. However, careful reading of Col. 18, lines makes clear that no encryption is done when the application package is sent via transmission media. With this fact in mind, it is clear that Uranaka et al. is in no way teaching or suggesting a method for ensuring security of a software product

	when it is "transmitted" between a server and a user. To further cement this fact, Uranaka et al. notes in column 18, lines 42-47, that security is maintained because "...use of the application package is limited to an owner of the IC card which stores a user secret key Sku..."
obtaining a title private key that is asymmetrically double encrypted by the server computer using the console public key and the user private key,	As noted above, the title software in Uranaka et al. is obtained over transmission media without security. Thus, Uranaka et al. could not teach using the user public key and the console public key.
use of the console public key created at the user computer defining a first layer of encryption, use of the user private key created at the server computer defining a second layer of encryption, the title private key and the title public key defining a title key pair; and	For the same reasons noted above, Uranaka et al. fails to teach this operation. Again, Uranaka et al. is teaches two methods. One is to send DVD's with previously encoded data (which is obtained from the user). It is true that Uranaka et al. teaches encoding user information on the DVDs, but that information is part of the control data that can be added after the manufacturing process. See Col. 18, lines 54-61.
decrypting the title public key encrypted software product using the title private key.	For at least the reasons given above, this step could not logically be taught by Uranaka et al. It is therefore respectfully submitted that the teachings of Schneier when combined with the teachings Uranaka et al. fail to suggest the aforementioned elements of the claimed invention.

In view of the above made comparisons and analysis of the primary reference, the Applicants respectfully request reconsideration and request a notice of allowance.

If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 749-6903. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SONYP007). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

Albert S. Penilla, Esq.
Reg. No. 39,487

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Facsimile: (408) 749-6901
Customer No. 25920